International Journal of Applied Engineering Research ISSN 0973-4562 Volume 15, Number 3 (2020) pp. 249-252

Secure Online Payment with Facial Recognition using MTCNN

Ms. Aria[1], Mr. Varun Agnihotri[2], Mr. Ankit Rohra[3], Mr. Rohit Sekhar[4]

[1] *MBA, Symbiosis Institute of Business Management, Bengaluru, Symbiosis University, Pune, India.*

[2] *MBA, Symbiosis Institute of Business Management, Bengaluru, Symbiosis University, Pune, India.*

[3] *MBA, Symbiosis Institute of Business Management, Bengaluru, Symbiosis University, Pune, India.*

[4] *MBA, Symbiosis Institute of Business Management, Bengaluru, Symbiosis University, Pune, India.*

Abstract

The recent advancements in technology have led to a surge in online transactions via online shopping, internet banking, payment gateways, etc. Security is the most prevailing issue during these transactions. Due to such issues people are hesitant to use online transactions, so we propose our system which secures online transactions using two-step verification. The first step is OTP verification followed by facial recognition. The system uses an online interface in order to interact with a user. The interface is used to get card details from the user. After the OTP verification, the user is authenticated using facial recognition. The system uses a MTCNN in order to verify the user by comparing the real time captured image of the user against the images associated with the users account.

Keywords: MTCNN, online payment, security, image verification, face recognition, credit card

1. INTRODUCTION

In the current world of advanced technology, it is easy for hackers to get personal details of users because of which some people are hesitant to use online transactions. This makes security an important factor at the time of making digital payments. Hence, we propose a system to enhance the security of online transactions by providing a 2-step verification process: OTP verification followed by Facial Recognition.

The system, which we will propose, will try to reduce the number of attacks at the time of making digital payments. Online transactions become vulnerable because of lost or stolen cards, account takeover, counterfeit cards, fraudulent application, multiple imprint, and collusive merchants. In the case of account takeover, a card holder unknowingly gives his banking details to a fraudster and the fraudster then makes a duplicate card with those details. Similarly, in counterfeit, a user's card is cloned and then used by the fraudster. Multiple imprints happen when the same singular transaction is recorded multiple times. In collusive merchants, employees of the merchant work with the fraudsters. The proposed system succeeds in reducing all these frauds by capturing and verifying a real time image of the card holders.

Biometric authenticity is gaining a lot of attention due to its uniqueness for every individual. Some of the various biometric authentications are fingerprint, hand geometry, iris, face and palm. In this paper, we are using face recognition as it's the most popular, easily usable and widely acceptable [8]. Under facial recognition, there are various techniques used like, SVM[2], PCA [2], LDA [3], CNN and MTCNN. This paper uses MTCNN for facial recognition as it has portrayed better results under facial recognition. Also, it is compatible with all operating systems and all types of browsers. The user (card holder) must simply have a have a camera connected to the device in order to capture a real time image, and a good internet connection to access the user interface (UI), as the system has a web UI.

2. 2. RELATED WORK

2.1 Techniques for securing online transactions

The existing methods of securing online transactions are account associated password, card verification value (CVV) and one-time password (OTP). OTP is a combination of alphabets and numbers which is sent to the account holders' registered phone number via SMS or via e-mail. Any card holder who doesn't have any of the 2 mentioned above will not be able to follow through with the online transaction. It is generally believed that OTP is secure and safe. However, it is not robust to attacks like impersonation, phishing, and malware-based replay attacks.

2.2 Techniques for biometrics

Biometric technology is used for authentication of a card holder. The various biometric techniques are using voice, face, palm and fingerprints. Voice recognition measures a user's voice patterns, speaking style and pitch, fingerprint identification uses patterns of the rides and valleys present in fingerprints scanned beforehand, palm identification uses palm prints and other physical traits for unique identification of user's palm, and face recognition captures and stores the facial features of an individual and stores them for identification process.

2.3 Techniques for face recognition

The different techniques used in facial recognition include PCA[2], SVM[2], LDA[3], CNN and MTCNN. Principle component analysis (PCA) is used to decrease the dimensionality of data to reduce the number of parameters in images, which are high dimensional correlated data. It is based on Eigen values and Eigen vectors. Support Vector Machine

(SVM) is used for binary classification. An SVM based classifier is used in facial recognition to predict the similarity and dissimilarity between two images[2]. Convolutional Neural Network is a deep neural network architecture which is used to extract features from images. CNNs can be used as classifiers or as feature extraction. Multi-task cascaded convolutional neural network is an algorithm consisting of 3 stages, which detects the bounding boxes of faces in an image along with their 5-Point Face Landmarks.

3. LITERATURE SURVEY

2.1 FaceNet (2015 IEEE): A Unified Embedding for Face Recognition and Clustering

In this paper is presented a system, called FaceNet [1]. FaceNet learns how to directly map face images to a compact Euclidean space. The distances between the generated vectors give the similarity between the faces. The created space can be used for different tasks such as face recognition, verification and clustering using standard techniques with FaceNet embeddings as feature vectors. We extend this concept to apply it to secure online transactions.

2.2 When Face Recognition Meets with Deep Learning (2015 IEEE)

The paper [4] aims to provide a common ground to all students and researchers alike by conducting an evaluation of easily reproducible face recognition systems based on CNNs. It uses public database LFW (Labelled Faces in the Wild) to train CNNs instead of a personal database. It proposes three CNN architectures which are the first reported architectures trained using LFW data. We use the LFW dataset to train our network as well as a personal database to test it.

2.3 Building Recognition System Based on Deep Learning (2016 IEEE)

Deep learning architectures use a multiple convolution layers and activation functions which are cascaded. The most important aspect is the setup-the number of layers and the number of neurons in each layer, the selection of activation functions and optimization algorithm. It [5] uses GPU implementation of CNN. The CNN is trained in a supervised way in order to achieve very good results. We extend this system in order to use it for the secure online transactions.

2.4 An Efficient Scheme for Face Detection (2015 IEEE)

This work [6] is based on skin colour, contour drawing and feature extraction to provide an efficient and simple way to detect human faces in images. The features under consideration are mouth, eyes, and nose. The results are with good accuracy, great speed and simple computations.

2.5 Gender and Age Classification of Human Faces (2017 IEEE)

This paper [10] introduces an approach to classify gender and age from images of human faces which is an essential part of our method for autonomous detection of anomalous human behaviour. This paper is a continuous study from previous research on heterogeneous data in which images as supporting evidence is used. A method for image classification based on a pre-trained deep model for feature extraction and representation followed by a Support Vector Machine classifier is presented. We use CNN in place of SVM.

2.6 Credit Card Transaction Using Face Recognition Authentication (2015 ICIIBMS)

This paper [8] is based on a credit card transaction system which integrates face recognition and face detection technology using Haar Cascade and GLCM algorithms. The training data set includes the extracted features from the images and is stored in administrator database, which is then used for the authentication. We use CNN instead to increase efficiency and reduce complexity of system.

3. SYSTEM ARCHITECTURE

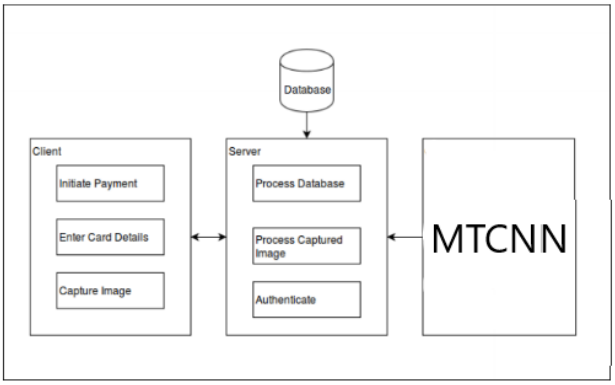


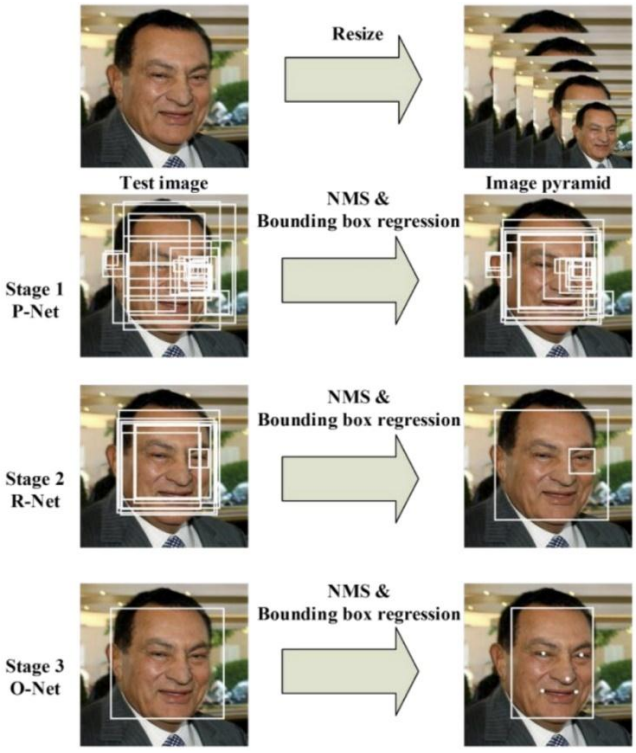
Fig -1: System Architecture

The system has the following components-Database, Client, Server and MTCNN. The database is divided into training and testing dataset. The training dataset, LFW, is used to train the MTCNN component while the testing dataset, a dataset of personal faces, is used to test its accuracy. The Server includes the modules used to interact with the database. They are also used to process the images received from the MTCNN. The Client side has the initiate payment, get card details and capture image modules. The capture image module is used to capture the image of the user and send it to the server side. The network uses a cascade structure with three networks; first the image is rescaled to a range of different sizes (called an image pyramid), then the first model (Proposal Network or P-Net) proposes candidate facial regions, the second model (Refine Network or R-Net) filters the bounding boxes, and the third model (Output Network or O-Net) proposes facial landmarks. [7] The system works as follows. A user initiates payment by entering the card

details in the displayed web page. The details are sent to server side and are authenticated. The user is then redirected to OTP web page. After entering a valid OTP, the user is redirected to the capture image web page where a real time image of user is captured and sent to server side. The image is processed via the MTCNN and authenticates the user against the image of the user stored in database at the server side.

4. METHODOLOGY

Multi Task Cascaded Convolutional Neural Network is being used for facial recognition and authentication of the user. MTCNN is a deep learning algorithm and is found to be efficient in analysing images because they use relatively little pre-processing compared to other image classification algorithms [4]. The network uses a cascade structure with three networks; first the image is rescaled to a range of different sizes (called an image pyramid), then the first model (Proposal Network or P-Net) proposes candidate facial regions, the second model (Refine Network or R-Net) filters the bounding boxes, and the third model (Output Network or O-Net) proposes facial landmarks. [7]



MTCNN is an algorithm with 3 stages, which detects the bounding boxes of faces in an image along with their 5 Point Face Landmarks. Each stage gradually improves the detection results by passing its inputs through a CNN, which returns candidate bounding boxes with their scores, followed by non max suppression.

In stage 1 the input image is scaled down multiple times to build an image pyramid and each scaled version of the image is passed through its CNN. In stage 2 and 3 we extract image patches for each bounding box and resize them (24x24 in stage 2 and 48x48 in stage 3) and forward them through the CNN of that stage. Besides bounding boxes and scores, stage 3 additionally computes 5 face landmarks points for each bounding box.

After fiddling around with some MTCNN implementations, it turns out that you can actually get quite accurate detection results at much lower inference times compared to CNN, even by running inference on the CPU.

5. RESULTS

The training of the MTCNN on our personal dataset of faces resulted in an accuracy of 80-85%. The system is able to correctly identify the users, on which the network has been trained, and authenticate them in the real time application.

6. CONCLUSION

The system enhances the security of online transactions by successfully recognizing and authenticating authorized users. The system can be used as a payment gateway for any application which requires online payments. These include ecommerce websites, internet and mobile banking. The system can be accessed on any operating system using any web browser. For future work, iris identification can be added to the system for further enhancing the security of the transactions.

ACKNOWLEDGEMENT

We would like to thank our guide, Prof. S.V. More, for her constant support and guidance. We would also like to express our deep gratitude to the principal, Dr. S.D. Lokhande, for his continuous efforts in creating a competitive environment in our college. We would like to convey our heartfelt thanks to our H.O.D., Prof. Wankhade, for giving us the opportunity to embark upon this topic. We also wish to thank all the staff members of the Department of Computer Engineering for helping us directly or indirectly in completing the work successfully.

REFERENCES

[1] Florian Schroff, Dmitry Kalenichenko,and James Philbin, “FaceNet: A Unified Embedding for Face Recognition and Clustering”, IEEE, 2015.

[2] Muzammil Abdulrahman, Alaa Eleyan, “Facial expression recognition using Support Vector Machines”, 23nd Signal Processing and Communications Applications Conference (SIU), IEEE, 2015.

[3] Yuan Wei, “Face Recognition Method Based on Improved LDA”, 9th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC), IEEE, vol. 2, pp. 456 - 459, 2017.

[4] Guosheng Hu, Yongxin Yang, Dong Yi,et. al.,When Face Recognition Meets with Deep Learning: an

Evaluation of Convolutional Neural Networks for Face Recognition, IEEE International Conference on Computer Vision Workshop, 2015.

[5] Pavol Bezak, "Building Recognition System Based on Deep Learning", IEEE, vol. 6, no. 1, pp. 212-217, 2016.

[6] Mohamed Heshmat, Moheb Girgis,et al, "An Efficient Scheme for Face Detection Based on Contours and Feature Skin Recognition", IEEE, 2015. [7] Kaipeng Zhang1 Zhanpeng Zhang2 Zhifeng Li1 Yu Qiao1, "Joint Face Detection and Alignment Using Multitask Cascaded Convolutional Networks.", IEEE Signal Processing Letters (SPL), vol. 23, no. 10, pp. 1499-1503, 2016 [8] Gittipat Jetsiktat, Sasipa Panthuwadeethorn, Suphakant Phimoltares, "Enhancing User Authentication of Online Credit Card Payment using Face Image Comparison with MPEG7-Edge Histogram Descriptor", International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS), IEEE, 2015.

[9] Adrian Rhesa Septian Siswanto, Anto Satriyo Nugroho, Maulahikmah Galinium, "Implementation of Face Recognition Algorithm for Biometrics Based Time Attendance System", International Conference on ICT for Smart Society (ICISS), IEEE, 2014.

[10] Xiaofeng Wang, Azliza Mohd Ali, Plamen Angelov, "Gender and Age Classification of Human Faces for Automatic Detection of Anomalous Human Behaviour", IEEE, 2017.

[11] W. Mohamed and M. Heshmat, M. Girgis, S. Elaw, A new method for face recognition using variance estimation and feature extraction, International Journal of Emerging Trends and Technology in Computer Science (IJETTCS), vol. 2, no. 2, pp. 134-141, 2013.

[12] R.S. Choras, "Facial feature detection for face authentication", in the Proceeding of IEEE Conference on Cybernetics and Intelligent Systems., 2013, pp.112-116, 2015.

[13] I. Aldasouqi and M. Hassan, Smart human face detection system, International Journal of Computers, vol. 5, no. 2, pp. 210-216, 2015. [14] A K. Jain, P. Flynn, A. A. Ross, Handbook of Biometrics, New York: Springer, 2010.